AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment comprising:

~~intercepting a Transmission Control Protocol (TCP) connection request by an application;~~

~~negotiating for a security association;~~

~~establishing the security association; and~~

~~allowing the TCP connection request to proceed after the security association is established.~~

monitoring application socket requests;

requesting a Transmission Control Protocol (TCP) connection by an application;

determining if there is an active IPsec security association that exists to protect network flow associated with the connection request;

preventing the connection request from proceeding to the TCP/IP layer if no active IPsec security association exists to protect the network flow;

determining if an IPsec security policy exists for the network flow if no active IPsec security association exists to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the IPsec security association based on the IPsec security policy if the IPsec security policy exists for the network flow; and

allowing the connection request to proceed if one of the active IPsec security association exists and the IPsec security association is established from the negotiation.

2. (Currently Amended) The method of claim 1, wherein the IPsec security association comprises an Internet Key Exchange (IKE) component.

3. (Currently Amended) The method of claim 1, wherein the IPsec security association is based on one or more of ~~the following~~:

a source Internet Protocol (IP) address;

a destination IP address;

a protocol;

a source port; and

a destination port.

4. (Currently Amended) The method of claim 3, wherein the protocol comprises one or more of ~~the following~~:

TCP;

User Datagram Protocol (UDP);

Internet Control Message Protocol (ICMP); and

Internet Group Management Protocol (IGMP).

5. (Cancelled)

6. (Currently Amended) The method of claim 1, further comprising retrieving the IPsec security association from a database.

7. (Currently Amended) The method of claim 6, wherein the database contains mappings between network flow information and the IPsec security association.

8. (Currently Amended) The method of claim 7, wherein the network flow information comprises one or more of ~~the following~~:

a source Internet Protocol (IP) address;

a destination IP address;

a protocol;

a source port; and

a destination port.

9. (Currently Amended) The method of claim 1, further comprising retrieving the IPsec security policy from the database.

10. (Currently Amended) A method for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment comprising:

monitoring application socket requests;

requesting transmission of ~~User Datagram Protocol (UDP)~~ data on a socket by an application;

~~intercepting the transmission of the UDP data on the socket by the application;~~

determining if the socket has been associated with an active IPsec security association;

determining if there is a defined IPsec security association that may be used to protect network flow if the socket has not been associated with an active IPsec security association;

determining what IPsec security policy should be used when negotiating ~~a~~ an IPsec security association for the network flow if there is no defined IPsec security association that may be used to protect the network flow;

preventing the data from being sent to the TCP/IP layer if there is no defined IPsec security association that may be used to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the IPsec security association if there is no defined IPsec security association that may be used to protect the network flow;

establishing the IPsec security association; and

allowing the ~~UDP~~ data to be sent in response to establishment of the IPsec security association.

11. (Previously Presented) The method of claim 10, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

12. (Currently Amended) The method of claim 10, comprising negotiating for the IPsec security association using IPsec security parameters specified by the IPsec security policy.

13. (Currently Amended) The method of claim 10, wherein the second determining comprises comparing filters with one or more of ~~the following~~:

a source Internet Protocol (IP) address;

a destination IP address;

a protocol;

a source port; and

a destination port, wherein the destination port includes one or more of ~~the following~~

a source Internet Protocol (IP) address,

a destination IP address,

a protocol,

a source port, and

a destination port related to the network flow.

14. (Currently Amended) The method of claim 13, wherein each filter comprises one or more of ~~the following~~:

a source Internet Protocol (IP) address;

a destination IP address;

a protocol;

a source port; and

a destination port.

15. (Currently Amended) The method of claim 13, wherein the IPsec security policy comprises at least one filter.

16. (Currently Amended) The method of claim 10, further comprising determining if the network flow can be allowed without the IPsec security association if no IPsec security policy exists for the network flow.

17. (Currently Amended) A system comprising:

a network;

a network interceptor between the application layer and the TCP/IP layer coupled with the network, the network interceptor to monitor an application's socket requests ~~intercept a Transmission Control Protocol (TCP) connection request by an application~~;

a security association database coupled to the network interceptor, the security association database containing a mapping of network flow information to Internet Protocol security (IPsec) security association information;

a security policy database coupled to the network interceptor, the security policy database containing policies that describe parameters that are to be used in a negotiation of an IPsec security association;

a security association negotiation component coupled with the network interceptor, the security association negotiation component to negotiate ~~a~~ an IPsec security association and to establish the IPsec security association; ~~and~~

the network interceptor to allow the TCP connection request to proceed after the IPsec security association is established; and

an (IPsec) packet classifier, the IPsec packet classifier responsible for performing IPsec processing on incoming and outgoing packets, wherein the network

interceptor insures that an IPsec security association is in place before allowing network traffic to flow between the application and the TCP/IP layer.

18. (Currently Amended) The system of claim 17, wherein the network flow information comprises one or more of ~~the following~~:

Internet Protocol (IP) addresses;

a protocol; and

ports.

19. (Cancelled)

20. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

~~intercept a Transmission Control Protocol (TCP) connection request by an application;~~

~~negotiate for a security association;~~

~~establish the security association; and~~

~~allow the TCP connection request to proceed after the security association is established.~~

monitor application socket requests;

request a Transmission Control Protocol (TCP) connection by an application;

determine if there is an active Internet Protocol security (IPsec) security association that exists to protect network flow associated with the connection request;

prevent the connection request from proceeding to the TCP/IP layer if no active IPsec security association exists to protect the network flow;

determine if an IPsec security policy exists for the network flow if no active IPsec security association exists to protect the network flow;

alert a security association negotiation component to initiate negotiation for an IPsec security association based on the IPsec security policy if the IPsec security policy exists for the network flow; and

allow the connection request to proceed if one of the active IPsec security association exists and the IPsec security association is established from the negotiation.

21. (Previously Presented) The machine-readable medium of claim 20, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

22. (Cancelled)

23. (Currently Amended) The machine-readable medium of claim 20, wherein the active IPsec security association comprises one or more of ~~the following~~:

a source Internet Protocol (IP);

a destination IP;

a protocol;

a source port; and

a destination port.

24. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

monitor application socket requests;

request transmission of ~~User Datagram Protocol (UDP)~~ data on a socket by the application;

~~intercept the transmission of the UDP data on the socket by the application;~~

determine if the socket has been associated with an active IPsec security association;

determine if there is a defined IPsec security association that may be used to protect network flow if the socket has not been associated with an active IPsec security association;

determine what IPsec security policy should be used when negotiating ~~a~~ an IPsec security association for the network flow if there is no defined IPsec security association that may be used to protect the network flow;

prevent the data from being sent to the TCP/IP layer if there is no defined IPsec security association that may be used to protect the network flow;

alert a security association negotiation component to initiate negotiation for the IPsec security association if there is no defined IPsec security association that may be used to protect the network flow;

establish the IPsec security association; and

allow the ~~UDP~~ data to be sent in response to establishment of the IPsec security association.

25. (Previously Presented) The machine-readable medium of claim 24, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

26. (Currently Amended) The machine-readable medium of claim 24, further cause the machine to negotiate for the IPsec security association using IPsec security parameters specified by ~~a~~ an IPsec security policy.

27. (Currently Amended) The machine-readable medium of claim 24, wherein the active IPsec security association comprises one or more of ~~the following~~:

a source Internet Protocol (IP);

a destination IP;

a protocol;

a source port; and

a destination port.

28-29. (Cancelled)

30. (New) The system of claim 17, wherein the IPsec security association comprises an Internet Key Exchange (IKE) component.